

(19)



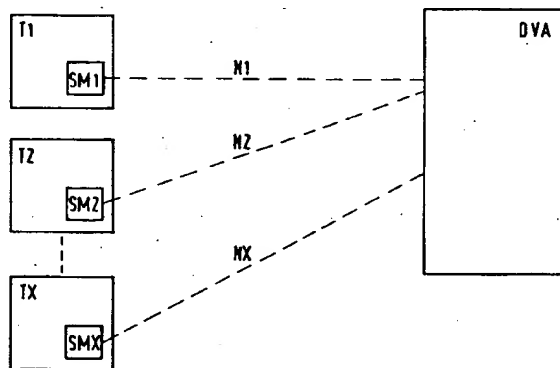
Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 649 080 A1**

(12)

EUROPÄISCHE PATENTANMELDUNG(21) Anmeldenummer: **94115873.5**(51) Int. Cl.⁶: **G06F 1/00**(22) Anmeldetag: **07.10.94**(30) Priorität: **15.10.93 DE 4335277**(43) Veröffentlichungstag der Anmeldung:
19.04.95 Patentblatt 95/16(84) Benannte Vertragsstaaten:
AT BE CH DE ES FR GB IT LI NL SE(71) Anmelder: **Siemens Nixdorf
Informationssysteme AG
Heinz-Nixdorf-Ring 1
D-33106 Paderborn (DE)**(72) Erfinder: **Hewel, Harald Dipl.-Ing.
Lilienstr. 22
D-86551 Aichach (DE)
Erfinder: Jost, Hildegard Dipl.-Math.
Gravelottestrasse 1a
D-81667 München (DE)
Erfinder: Kruse, Dietrich Dipl.-Ing.
Ulmenstrasse 9
D-85521 Ottobrunn (DE)**(74) Vertreter: **Fuchs, Franz-Josef, Dr.-Ing. et al
Postfach 22 13 17
D-80503 München (DE)**(54) **Verfahren zur Sicherung sicherheitsrelevanter Informationen.**

(57) Sicherheitsrelevante Informationen, wie beispielsweise kryptografische Schlüssel, sind im Sicherheitsmodul (SM) eines Terminals gespeichert. Das Terminal (T) ist mit einer zentralen Datenverarbeitungsanlage (DVA) gekoppelt. Vor einem Datenaustausch zwischen Terminal (T) und Datenverarbeitungsanlage (DVA) erfolgt eine Authentifikation. Bei dieser Authentifikation teilt das Sicherheitsmodul (SM) der Datenverarbeitungsanlage (DVA) einen Zeitabstand in verschlüsselter Weise mit, nach dessen Ablauf eine nochmalige Authentifikation von der Datenverarbeitungsanlage (DVA) anzustoßen ist. Wird diese nochmalige Authentifikation nicht rechtzeitig angestoßen, werden die im Sicherheitsmodul (SM) enthaltenen sicherheitsrelevanten Informationen gelöscht.


EP 0 649 080 A1

Die Erfindung betrifft ein Verfahren zur Sicherung sicherheitsrelevanter Informationen in einem mit einer zentralen Datenverarbeitungsanlage gekoppelten Sicherheitsmodul eines Terminals. Solche Sicherheitsmodule werden in Terminals zur Absicherung der Datenübertragung eingesetzt, wenn Anwendungen im militärischen Bereich, im Bankwesen oder ganz allgemein im Bereich der elektrischen oder optischen Übertragung von personenbezogenen oder sonstigen zu schützenden Daten vorgesehen sind. Sicherheitsrelevante Informationen sind beispielsweise kryptografische Schlüssel.

Es sind bereits verschiedene Methoden bekannt, mit denen die sicherheitsrelevanten Informationen in einem Sicherheitsmodul geschützt werden können. Eine einfache aber unpraktikable Möglichkeit ist es, die Sicherheitsmodule nur unter Aufsicht von Sicherheitspersonal zu verwenden und bei Nichtbenutzung die Sicherheitsmodule in einem Tresor wegzuschließen. Weitere Möglichkeiten sind aus einem Prospekt der Firma GAO mbH mit dem Titel "EFT-POS-Terminal" bekannt. Dort ist beschrieben, die sicherheitsrelevanten Bestandteile, die die sicherheitsrelevanten Informationen enthalten, mit einer vergußmasse zu überdecken, das Sicherheitsmodul vollständig mit einem Gehäuse zu umschließen und durch einen Lichtsensor sicherzustellen, daß die sicherheitsrelevanten Informationen bei Einfall von Licht in das Gehäuse gelöscht werden. Ferner ist aus DE 41 15 703 bekannt, Leiterstrukturen am Gehäuse des Sicherheitsmoduls vorzusehen, die bei mechanischer Beeinträchtigung das Löschen sicherheitsrelevanter Informationen bewirken. Ferner ist es bekannt, die sicherheitsrelevanten Daten bei Spannungsausfall oder Unterschreiten einer Schwellenspannung oder Veränderung des Systemtaktes zu löschen. Die sicherheitsrelevanten Daten können auch durch einen logischen Zugriffsschutz, mit dessen Hilfe ein Auslesen der sicherheitsrelevanten Daten im Klartext verhindert wird, geschützt werden.

Die bekannten Schutzmaßnahmen sind jedoch nicht in der Lage, bei einem möglichen Diebstahl des Sicherheitsmoduls aus dem Terminal ein zuverlässiges Löschen der sicherheitsrelevanten Informationen im Sicherheitsmodul zu gewährleisten. Werden Spannungs- und Taktversorgung aufrechterhalten, kann das Sicherheitsmodul mit den sicherheitsrelevanten Daten aus dem Einflußbereich des Terminals entfernt werden.

Der vorliegenden Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren zur Sicherung sicherheitsrelevanter Informationen in einem mit einer zentralen Datenverarbeitungsanlage gekoppelten Sicherheitsmodul eines Terminals aufzuzeigen, das ein Entfernen des Sicherheitsmoduls aus dem Einflußbereich der Datenverarbeitungsanlage ein-

schließlich der im Sicherheitsmodul enthaltenen sicherheitsrelevanten Informationen zuverlässig verhindert.

Diese Aufgabe wird durch die im Patentanspruch 1 angegebenen Merkmale gelöst. Bei Überschreitung des Zeitabstandes zur Wiederholung der Authentifikationsprozedur werden die sicherheitsrelevanten Informationen trotz Vorliegen anderer Bedingungen, wie beispielsweise korrekte Versorgungsspannung und Taktfrequenz, gelöscht. Der Versuch, die sicherheitsrelevanten Informationen in einer ungesicherten Umgebung aus dem Sicherheitsmodul auszulesen, kann dadurch wirksam verhindert werden.

Ausgestaltungen und Weiterbildungen der Erfindung sind in Unteransprüchen angegeben. Ein Ausführungsbeispiel der Erfindung wird im folgenden anhand der Zeichnung näher erläutert.

Die Figur zeigt ein Blockschaltbild mehrerer, mit einer Datenverarbeitungsanlage verbundener Terminals.

An eine zentrale Datenverarbeitungsanlage DVA sind eine Mehrzahl von Terminals T1, T2...Tx gekoppelt. Die Koppelung erfolgt mittels privater oder öffentlicher Nachrichtennetze N1, N2...Nx. Die Terminals T1, T2...Tx sind jeweils einem Anwender zugeordnet. Zur Sicherung des Datenverkehrs von einem Anwender zur zentralen Datenverarbeitungsanlage DVA sind in den Terminals T1, T2...Tx jeweils anwenderspezifische Schlüssel enthaltende Sicherheitsmodule SM1, SM2...SMx vorgesehen. Die Datenverarbeitungsanlage DVA akzeptiert nur Terminals T1, T2...Tx mit Sicherheitsmodulen SM1, SM2...SMx, die sich erfolgreich gegenüber der Datenverarbeitungsanlage DVA authentifizieren können. Die Authentifikation erfolgt, wie beispielsweise aus dem Artikel "Chipkarten praktisch und sicher", Telematik Magazin 1/1988, Seite 8 bis 12 bekannt, durch gegenseitigen Austausch verschlüsselter Informationen nach der "Challenge and Response-Methode". Entsprechendes gilt auch umgekehrt. Ein Sicherheitsmodul SM akzeptiert nur eine Datenverarbeitungsanlage DVA, die sich auch erfolgreich gegenüber dem Sicherheitsmodul SM authentifiziert.

Bei jeder Authentifikation teilt das Sicherheitsmodul SM der Datenverarbeitungsanlage DVA einen beispielsweise von einem Zufallsgenerator im Sicherheitsmodul SM bestimmten Zeitabstand mit, an dem eine weitere Authentifikationsprozedur durchgeführt werden soll. Eine Authentifikationsprozedur wird grundsätzlich von der Datenverarbeitungsanlage DVA angestoßen. Ein Start der Authentifikationsprozedur von Seiten eines Sicherheitsmoduls SM ist demnach unmöglich.

Zusätzlich zum Zeitabstand teilt das Sicherheitsmodul SM der Datenverarbeitungsanlage DVA die Dauer eines Zeitfensters mit, in das der nach-

folgende Anstoß zum Ablauf der Authentifikationsprozedur fallen muß. Die Lage dieses Zeitfensters zum festgelegten Zeitabstand und die absolute Länge des Zeitfensters wird jeweils zufällig beispielsweise durch einen Zufallsgenerator des Sicherheitsmoduls SM bestimmt.

Das Sicherheitsmodul SM überwacht mit Hilfe einer im Sicherheitsmodul SM enthaltenen Zeitbasis die Einhaltung des Zeitabstandes und des Zeitfensters zum Anstoß einer Authentifikationsprozedur. Wird diese Authentifikationsprozedur nicht im vorgegebenen Zeitfenster angestoßen, veranlaßt die Steuerung des Sicherheitsmoduls SM das Löschen der sicherheitsrelevanten Informationen. Das Sicherheitsmodul SM ist dann unbrauchbar und kann nur in gesicherter Umgebung, beispielsweise beim Netzbetreiber der Datenverarbeitungsanlage DVA, wieder mit sicherheitsrelevanten Informationen versorgt und damit funktionsfähig gemacht werden.

Da die vom Sicherheitsmodul SM festgelegten Zeitabstände und Zeitfenster aufgrund der verschlüsselten Übertragung zur Datenverarbeitungsanlage DVA nur der Datenverarbeitungsanlage DVA bekannt sind und aufgrund der zufälligen Bestimmung auch nicht vorhersehbar sind, ist es bei Entfernen des Sicherheitsmoduls SM aus dem Terminal T und damit einer Trennung von der Datenverarbeitungsanlage DVA nicht möglich, die sicherheitsrelevanten Informationen dauerhaft im Sicherheitsmodul SM zu erhalten. Ein unberechtigtes Benutzen des Sicherheitsmoduls SM, das unter Beibehaltung der Spannungs- und Taktversorgung aus dem Terminal gestohlen wurde, ist damit zeitlich beschränkt.

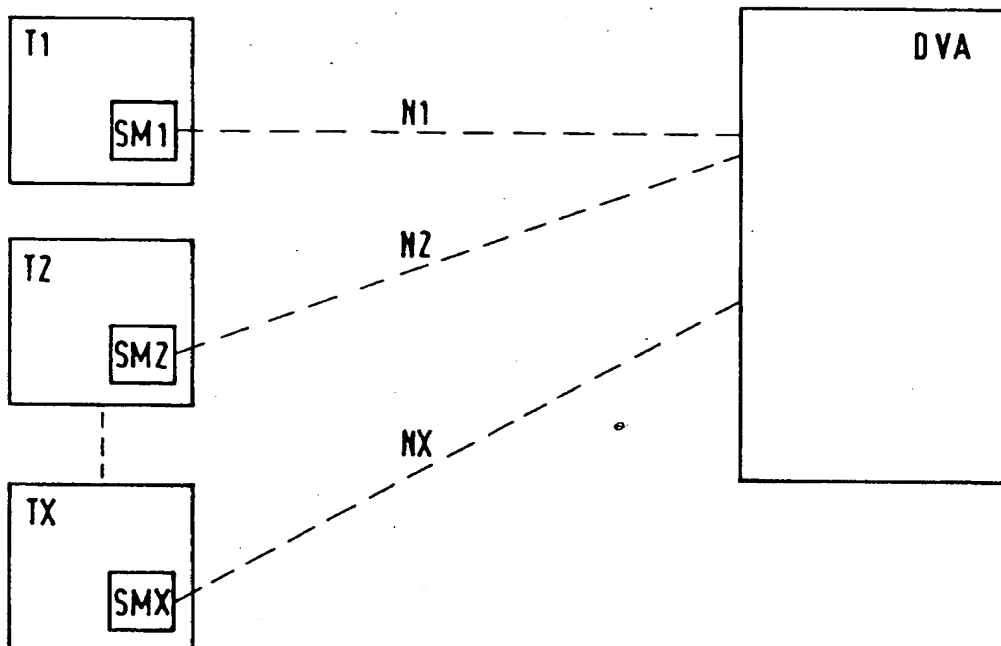
Patentansprüche

1. Verfahren zur Sicherung sicherheitsrelevanter Informationen in einem mit einer zentralen Datenverarbeitungsanlage (DV) gekoppelten Sicherheitsmodul (SM) eines Terminals (T), mit einer

- von der Datenverarbeitungsanlage (DVA) angestoßenen Authentifikation zwischen dem Sicherheitsmodul (SM) und der Datenverarbeitungsanlage (DVA),
- Wiederholung der Authentifikation in einem vom Sicherheitsmodul (SM) des Terminals (T) bestimmten, der Datenverarbeitungsanlage (DVA) bei der vorhergehenden Authentifikation übermittelten Zeitabstand, und
- Zerstörung der sicherheitsrelevanten Information im Sicherheitsmodul (SM) bei negativem Authentifikationsverlauf und/oder Überschreitung des der Datenverarbeitungsanlage (DVA) mitgeteilten

Zeitabstandes.

2. Verfahren nach Anspruch 1 mit einer vom Sicherheitsmodul (SM) des Terminals (T) bestimmten, der Datenverarbeitungsanlage (DVA) gemeinsam mit dem Zeitabstand mitgeteilten Zeitfenster, während der die Wiederholung der Authentifikationsprozedur von der Datenverarbeitungsanlage (DVA) anzustoßen ist.
3. Verfahren nach einem der Ansprüche 1 oder 2, mit einer jeweils zufälligen Bestimmung des Zeitabstandes und/oder des Zeitfensters durch das Sicherheitsmodul (SM).
4. Verfahren nach einem der vorhergehenden Ansprüche, mit einer verschlüsselten Übermittlung des Zeitabstandes und/oder Zeitfensters vom Sicherheitsmodul (SM) zur Datenverarbeitungsanlage (DVA).





Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 94 11 5873

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
X	US-A-4 882 752 (LINDMAN ET AL) * Zusammenfassung; Abbildungen 1,3,5 * * Spalte 2, Zeile 65 - Spalte 3, Zeile 13 * * Spalte 3, Zeile 39 - Spalte 4, Zeile 41 * * Spalte 10, Zeile 16 - Zeile 62 * * Spalte 11, Zeile 29 - Zeile 45 * * Ansprüche 1,2 *	1,2	G06F1/00
Y	---	3,4	
Y	US-A-5 189 700 (BLANDFORD) * Zusammenfassung; Abbildung 1 * * Spalte 2, Zeile 3 - Zeile 21 * * Spalte 3, Zeile 12 - Zeile 21 *	3,4	
A	PTR PHILIPS TELECOMMUNICATIONS AND DATA SYSTEMS REVIEW, Bd.47, Nr.3, September 1989, HILVERSUM, NL; Seiten 1 - 19 R.C.FERREIRA 'The Smart Card: A High Security Tool in EDP' * Abbildung 4 * * Seite 5, Zeile 6 - Seite 7, Spalte 5 *	4	
			RECHERCHIERTE SACHGEBIETE (Int.Cl.6)
			G06F H04L
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenamt DEN HAAG		Abschlußdatum der Recherche 30. Januar 1995	Prüfer Powell, D
KATEGORIE DER GENANNTEN DOKUMENTE			
X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : nichtschriftliche Offenbarung P : Zwischenliteratur T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus andern Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument			

EPO FORM 1503 03.92 (P04 C03)

This Page Blank (uspto)